Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

070.203 Security Exceptions and Exemptions to CHFS OATS Policies and Security Controls Policy

Version 2.2
October 1, 2018

Revision History

Date	Version	Description	Author
3/1/2005	1.0	Effective Date	CHFS OATS Policy Charter Team
10/1/2018	2.2	Review Date	CHFS OATS Policy Charter Team
10/1//2018	2.2	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or designee)	10/1/2018	Jennifer Harp	Jennifer L. Harp
CHFS Chief Information Security Officer (or designee)	10/1/2018	DENNIS E. LEBER	D. E.

Table of Contents

1 Policy Definitions

- **Addition:** A request that is considered to be an addition, need to be added as new, to the Enterprise Architectural Standards.
- **Application:** A software program designed to perform a specific function (e.g., Partner Portal, Benefind, etc.).
- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Database (server or components):** A Database Management System (DBMS) is a computer software application that interacts with the user, other applications, and the database itself to capture and analyze data. A general-purpose DBMS is designed to allow the definition, creation, querying, update, and administration of databases.
- **Electronic Personal Health Information (ePHI):** Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form.
- **Exception:** A request considered a short-term solution to issues relating to Security Policies and Controls or Enterprise Architectural Standards that must be reviewed and/or renewed annually.
- **Exemption:** A request that is considered to be a longer term solution to issues relating to Security Policies and Controls or Enterprise Architectural Standards that must be reviewed for accuracy and need on an annual basis.
- **Federal Tax Information (FTI):** Information received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service, that includes tax information. Examples would be an individual’s tax return or anything that the IRS collects and that the IRS is going to use in order to determine a person's tax liability or potential tax liability.
- **Modification:** A request considered an update to any existing Enterprise Architectural Standards.
- **Network Components:** Hardware or software (virtualized) components that perform networking or communication functions, control access, manage incoming or outgoing network traffic, monitor for spam or malicious content (e.g., routers, firewalls, switches, Intrusion Detection System/Intrusion Protection System (IDS/IPS), web or email gateways, or vendor appliances).

- **Operating System:** Software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.
- **Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual's identity (i.e. name, Social Security number, biometric records, etc.). PII can be the individual's personal information or is identified when combined with other personal or identifiable information (i.e. date of birth, birth place, mother's maiden name, etc.).
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.
- **Web Server:** A computer that runs a Web site. Using the Hypertext Transfer Protocol (HTTP), the Web server delivers Web pages to browsers as well as other data files to Web-based applications (e.g., Internet Information Server (IIS), or Apache).

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS must establish a comprehensive level of security controls through an exception/exemption policy. CHFS contract, state, and vendor staff/personnel are provided procedures, guidance and documentation required, via this policy, to submit exception and exemption requests.

2.2 Scope

The scope of this process applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This process covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Advisor have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft(s) of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with organizations and/or agencies with the cabinet, which access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible to adhere to this policy. This individual is responsible for the acknowledgement that due diligence has been taken to reduce risk, justify the need for the exception, exemption, etc. is provided, and that the proposal addresses the risk as best of ability and current information at the time of the request. This reviewer does not approve any risks being accepted by the business, rather acknowledges the security around the risk being requested for acceptance, and the information provided gives the approver a clear understanding of the risk they are accepting and approving.

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

3.3 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

3.4 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section 8 Policy References below that pertain to the agency’s applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).CHFS OATS Requestor.

3.5 CHFS OATS Requestor

This role/user is responsible to provide the business justification; explanation of risk involved/being accepted, mitigation plan/controls in place to reduce the risk, etc. for the exception/exemption request. This contact will be ultimately responsible for following the request through the approval process. This individual will have the responsibility to review and resubmit an exception/exemption annually as deemed necessary.

3.6 CHFS OATS Branch Manager (BM)

This role/approver is responsible for reviewing and approving the initial accuracy and need of the data and risk(s) presented for the exception or exemption. This individual will be responsible to ensure the requestor reviews and resubmits an exception/exemption annually as deemed necessary.

3.7 CHFS OATS Information Security (IS) Team

The IS Team is responsible for acknowledging that the requested exception/exemption is justified by a business need, and recommends possible other solutions for which the requestor may not be aware. This role also ensures that the solution proposed contains detailed information, so that the approver is aware of the risks, and can make an informed accept/reject decision. In addition, the IS Team is responsible for ensuring that any security concerns to be communicated for consideration at the time of the request.

3.8 CHFS OATS Technical Architect (TA) Group

This role/reviewing unit is responsible for the acknowledgement that no major technical or operational concerns are present at the time of exception/exemption request. This reviewing unit does not approve any risks accepted by the business, rather acknowledges that the technical and operational information provided a clear understanding of the risk(s) the approvers will be accepting and approving. This reviewing unit also identifies if there are technical solutions that may be available which removes the need to request an exception or exemption.

3.9 CHFS OATS Division Director (DD)

This role/approver is responsible for reviewing and approving the accuracy of the need, data, and risk(s) presented for the exception/exemption.

3.10 CHFS OATS Executive/Deputy Executive Director/System Owner

This approver is ultimately responsible for reviewing, approving, and accepting the risk(s) presented for the exception/exemption, if the request deals only with the system.

3.11 CHFS Business Approval Unit/Data Owner

This approver(s) is ultimately responsible for reviewing, approving, and accepting the risk(s) presented for the exception/exemption, if the request relates or involves agency data.

4 Policy Requirements

4.1 General

CHFS OATS management and OATS IS Team must review, acknowledge, and/or approve any deviations from CHFS OATS Policies and Security Controls.

Requests for exceptions or exemptions to OATS Policies and Security Controls must be completed using the CHFS Security Exception and Exemption Request SharePoint. Help with how to complete a security exception/exemption on the SharePoint can be found within the CHFS Security Exception and Exemption Requests Process.

Once a requestor completes a request in SharePoint, it is sent via a workflow for management and security review and approval. At a minimum, each request shall have the following information completed by the requestor:

- Agency for whom the exception is being requested
- Date required by
- Request type (i.e. Exception, Exemption, Addition, Modification)
- Applicable NIST Security Control Families
- Explanation of the Request
- Business Justification/Reason
- Explanation of Risk to be Accepted
- Risk Mitigation Plan/Explanation of Mechanisms for Compliance (or Risk Analysis/Assessment)

Through the SharePoint workflow, the request reviewed and approved by the applicable CHFS OATS Branch Manager. Following the branch manager approval, the CHFS OATS IS Team, Chief Information Security Officer (CISO) and CHFS OATS Technical Architect (TA) Group/Chief Technical Officer (CTO) shall acknowledge the exception or exemption request. Then the CHFS OATS Division Director and the CHFS OATS Executive/Deputy Executive Director review and provide final approval for the request.
Recommended to submit requests for exceptions or exemptions to the CHFS/OATS Policies and Security Controls at least one (1) business week prior to the request needs. This is to ensure approvers have adequate time to research and review the request for approval.

Exceptions and/or exemptions will be applicable for a maximum of one (1) year. Exceptions must be reviewed and resubmitted for approval annually while exemptions must be reviewed for accuracy and need annually as deemed necessary. The CHFS Security Exception and Exemption Request SharePoint will be the repository for of all exceptions requested and granted.

Any exception, addition, or modification request related to the Enterprise Architecture and Kentucky Information Technology Standards (KITS) Library, requires approval from the Information Technology Standards Committee (ITSC). If a request is required, it must be submitted by a CHFS Authorized Agency's IT Services Contact, using either the Exception Request Form, COT-F027 paper form, or via the COT ITSC Exception/Addition/Modification Request SharePoint site.

Requests that require ITSC approval must be submitted with at least two (2) business weeks to allow adequate time for consideration, and to obtain the required signatures.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

There are no exceptions to this policy.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS Authorized Agency's IT Services Contact
- CHFS OATS Policies List
- CHFS OATS Standards List
- CHFS OATS Process: CHFS Security Exception and Exemption Requests Process
- CHFS OATS Exception/Exemption SharePoint Roles
- CHFS Security Exception and Exemption Request SharePoint
- COT ITSC Exception/Addition/Modification Request SharePoint
- Enterprise IT Policies
- Enterprise Architecture and Kentucky Information Technology Standards (KITS) Library
- Enterprise IT Form: Exception Request Form, COT-F027
- Enterprise IT Form: Enterprise Security Exemption Request, COT-F085
- Health Insurance Portability and Accountability Act of 1996 (HIPAA):
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule: 45CFR164.308(a)(1)(ii)(A)
- Internal Revenue Services (IRS) Publications 1075

- Kentucky Revised Statute (KRS) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- National institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Moderate Security Control Family Descriptions
- Social Security Administration (SSA) Security Information